Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合

Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合

Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合

表 *1:* 機能の履歴

機能名	リリース情報	機能説明
Cisco Secure Equipment Access との統合	Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a Cisco Catalyst SD-WAN Manager リリース 20.16.1	Cisco Secure Equipment Access（SEA）は、ネットワーク接続されたアセットへのリモートアクセスを提供するソリューションです。アセットには、サーバー、Industrial Internet of Things（IIoT）デバイスなど、IP アドレスによって到達可能なものをすべて含めることができます。 Cisco Catalyst SD-WAN との統合により、Cisco SD-WAN Manager を使用して Cisco Catalyst SD-WAN ネットワーク内に Cisco SEA ソリューションを展開できるようになります。

Cisco Secure Equipment Access との統合に関する情報

Cisco Secure Equipment Access（SEA）は、ネットワーク接続されたアセットへのリモートアクセスを提供するソリューションです。アセットには、サーバー、Industrial Internet of Things（IIoT）デバイスなど、IP アドレスによって到達可能なものをすべて含めることができます。Cisco Catalyst SD-WAN との統合により、Cisco SD-WAN Manager を使用して次のことが可能になります。

- Cisco Catalyst SD-WAN オーバーレイネットワーク内にあるルータなどのデバイスに SEA エージェントをインストールする
- オーバーレイネットワーク内のデバイスと Cisco Secure Equipment Access クラウドポータル間の接続を設定する
- リモートアセットがデバイスに接続する方法を設定する

デバイスに SEA エージェントをインストールして、ここで説明した接続を設定すると、他のリモートアクセスタスクは Cisco SEA に対して通常どおり動作します。Cisco DevNet サイトの「Secure Equipment Access Overview」[英語] を参照してください。

Cisco Secure Equipment Access との統合のメリット

時間とコストのかかるサイト訪問を行うことなく、運用テクノロジー（OT）のアセットを設定、管理、障害対応するためには、リモートアクセスが欠かせません。Cisco Secure Equipment（SEA）は、ゼロトラストネットワークアクセス（ZTNA）ソリューションのすべてのメリットと、運用環境への大規模展開を簡素化するネットワークアーキテクチャを融合したものです。インストールと管理のための専用ハードウェアや、設定と保守を行うための複雑なファイアウォールルールはありません。包括的なセキュリティ機能、高度なサイバーセキュリティ制御、アイデンティティとコンテキストに基づき簡単に作成できるポリシーを備えています。

Cisco SEA には、次に示すような多くのメリットがあります。

- 運用の効率化

  運用チームは、OT アセットが NAT 境界の背後にある場合でも簡単にリモートアクセスできます。

- シンプルな設置と拡張性

  既存のルータやスイッチを使用して運用するため、専用アプライアンスや複雑なファイアウォール設定は必要ありません。

- 強力なセキュリティ制御

  MFA と SSO でユーザーを認証します。Cisco SEA は、各ユーザーのセキュリティ態勢を検証し、関連するアセットへのアクセスのみを提供します。

- 最小権限アクセス

  特定のプロトコルのみを使用し、指定された時間にのみ特定のデバイスにアクセスすることを厳選されたユーザーに許可します。

- 監査証跡

  セッションを記録し、調査とコンプライアンスのために監査証跡を作成します。

Cisco Secure Equipment Access アプリケーション

SEA エージェントのインストール

Cisco Secure Equipment Access（SEA）エージェントと呼ばれる Cisco IOx アプリケーションは、デバイス（ネットワーク内のルータ）に Cisco SEA の機能を提供します。Cisco SD-WAN Manager を介してデバイスで Cisco SEA を有効にすると、デバイスでは Cisco SEA アプリケーションがダウンロード後にインストールされます。

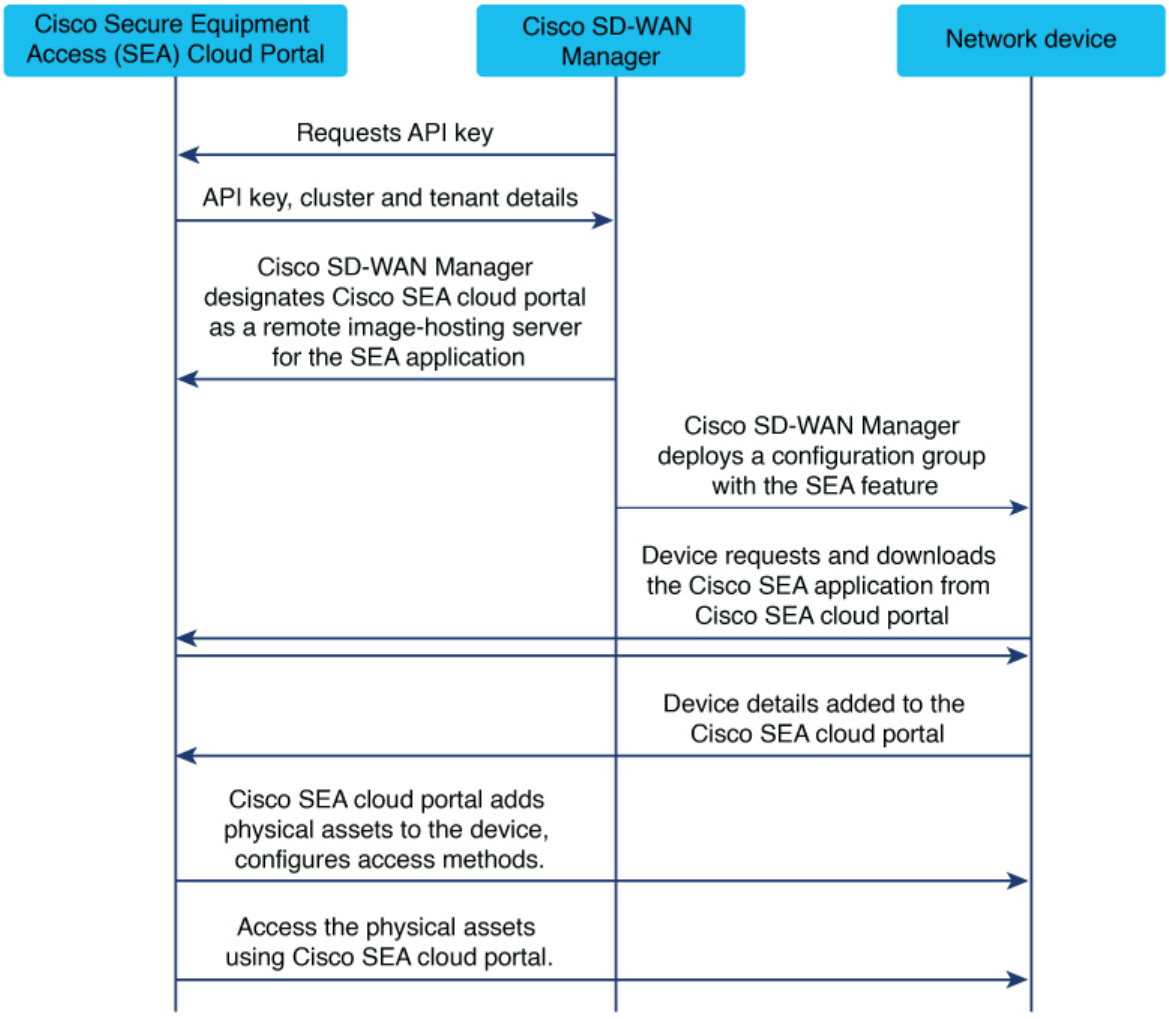
Cisco SEA クラウドポータル

Cisco SEA エージェントのインストールが正常に完了すると、デバイスは Cisco SEA クラウドポータルと通信します。通信するデバイスは、Cisco SEA クラウドポータルのデバイスリストに表示されます。

Cisco Secure Equipment ソリューションへのオンボードプロセス

オンボードプロセスの概要

図 *1 : Cisco Secure Equipment Access と Cisco Catalyst*



の統合

1. 接続を確立するための API キーの取得

ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定 （8 ページ）の手順の前提条件に従い Cisco SEA クラウドポータルにログインして、API キーを生成します。

2. Cisco SEA アプリケーションのイメージホスティング サーバーの指定

   ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定 （8 ページ）の手順を完了すると、Cisco SD-WAN Manager では API キー情報に基づいて、Cisco SEA クラウドポータルが Cisco SEA アプリケーションのリモートイメージ ホスティング サーバーとして指定されます。

   アプリケーションのダウンロード元のホストとして Cisco SEA を指定するために、Cisco SD-WAN Manager では Cisco SEA クラウドポータルがリモートサーバーとして追加されます。追加されると、**[Maintenance]** > **[Software Repository]** ページの [Remote server] タブに表示されます。Cisco Secure Equipment Access との統合に関するガイドライン （7 ページ）で説明されているように、このサーバーは編集または削除しないでください。

3. Cisco SEA アプリケーションのダウンロード

   Cisco SEA の設定をネットワーク内のデバイスにプッシュすると、デバイスが Cisco SEA クラウドポータルに接続されて、Cisco SEA アプリケーションがダウンロードされます。

4. アプリケーションのアクティブ化

   デバイスではアプリケーションがインストールされた後に、アクティブ化されます。これにより、デバイスが Cisco SEA ソリューションの一部として機能できるようになります。

Cisco Secure Equipment Access ソリューションの利用

ここで説明する手順を実行すると、デバイスを Cisco Secure Equipment Access ソリューションの一部として機能させることができます。この設定が完了したら、Cisco SEA を使用してリモートアセットへのアクセスを管理します。詳細については、Cisco DevNet サイトの Cisco Secure Equipment Access のマニュアル [英語] を参照してください。

Cisco Secure Equipment Access との統合でサポートされるプラットフォーム

表 *2:* サポートされるプラットフォーム

プラットフォーム シリーズ	モデル
Cisco Catalyst IR1100 高耐久性シリーズ ルータ	Cisco Catalyst IR1101

プラットフォーム シリーズ	モデル
Cisco Catalyst IR1800 高耐久性シリーズ ルータ	Cisco Catalyst IR1821 Cisco Catalyst IR1831 Cisco Catalyst IR1833 Cisco Catalyst IR1835

Cisco Secure Equipment Access との統合の前提条件

Cisco Secure Equipment Access ポータルへのネットワーク到達可能性

Cisco SEA 機能を追加した設定グループを展開する前に、Cisco SEA エージェント アプリケーションを実行するネットワーク内のルータが Cisco SEA クラウドポータルにネットワーク経由で到達できることを確認してください。

この要件があるため、デバイスと Cisco SEA を連携させるための設定は、次の 2 段階のプロセスになります。

1. 設定グループを一連のデバイスに展開して、Cisco SEA クラウドポータルへの到達可能性を確立します。
2. 設定グループを一連のデバイスに展開して、デバイスで Cisco SEA を有効にします。

   前の手順で到達可能性を確立したら、その手順で使用したものと同じ設定グループを変更して Cisco SEA 機能を追加し、その設定グループをデバイスに展開できます。

Cisco SEA 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco SEA クラウドポータルへの到達可能性を確立します。

仮想ポート グループ インターフェイス

Cisco SEA アプリケーションでは、仮想ポートグループ（VPG）インターフェイス 7 ～ 10 が使用可能である必要があります。これらの VPG インターフェイスが別のアプリケーションで使用するように設定されていないことを確認してください。

Cisco SEA アプリケーションは、Cisco SEA クラウドポータルに接続するために VPG インターフェイス 7 を使用し、リモートアセットに接続するために VPG インターフェイス 8 ～ 10 を予約します。仮想ポートグループに適用される制限については、Cisco Secure Equipment Access との統合に関する制限事項 （7 ページ）を参照してください。

仮想ポート グループ インターフェイス 7 の IP アドレス

Cisco SEA クラウドポータルに VPG インターフェイス 7 を接続するための IP アドレスをルータごとに設定します。

Cisco Secure Equipment Access との統合に関するガイドライン

リモートサーバーは削除しないでください

Cisco SD-WAN Manager では、Cisco SEA ポータルインスタンスが**[Maintenance]** > **[Software Repository]**ページの [Remote server] タブにサーバーとして追加されます。

これらのリモートサーバーは編集または削除しないでください。

Cisco Secure Equipment Access との統合に関する制限事項

単一の Cisco SEA クラウドポータル

Cisco SD-WAN Manager は、単一の Cisco SEA クラウドポータルにのみ接続できます。

単一の Cisco SD-WAN Manager

Cisco SEA クラウドポータルで定義されているように、1 つの組織は 1 つの Cisco SD-WAN Manager にのみ接続できます。Cisco SD-WAN Manager インスタンスは単一の組織を表すため、これはマルチテナント環境で動作する Cisco SEA クラウドポータルに影響を及ぼします。

仮想ポートグループ（VPG）およびリモートアセット接続

Cisco SEA アプリケーションは、Cisco SEA クラウドポータルに接続するために VPG インターフェイス 7 を使用し、アセットに接続するために VPG インターフェイス 8 ～ 10 を予約します。単一の VPG インターフェイス（8、9、10 のいずれか）は、単一のリモートアセットネットワークへの接続を提供できます。リモート アセット ネットワークには、複数のアセットを含めることができます。

Cisco Secure Equipment Access との統合の設定（概要）

手順

ステップ 1 ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定 （8 ページ）
ステップ 2 SEA 機能を使用した設定グループプロファイルの作成 （9 ページ）
ステップ 3 設定グループへの Cisco SEA 機能の追加 （13 ページ）
ステップ 4 Cisco SEA 機能を追加した設定グループの展開 （13 ページ）

次のタスク

設定手順が完了すると、デバイスで実行されている Cisco SEA アプリケーションのアクティビティをモニターできます。デバイス上の Cisco Secure Equipment Access アプリケーションのモニター （16 ページ）を参照してください。

ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定

始める前に

- API キー

  Cisco SEA クラウドポータルで API キーを作成して、デバイスが Cisco SEA クラウドポータルとセキュアなリンクを確立できるようにします。

  API キーの作成の詳細については、Cisco DevNet サイトの Cisco Secure Equipment Access のマニュアル [英語] を参照してください。API キーを生成する際、外部コントローラと統合するためのキーを有効にするオプションがある場合は、そのオプションを選択します。

  API キーをコピーして、手順で使用できるように準備しておきます。

- 接続

  Cisco SEA と連携するネットワーク内のデバイスは、ネットワークを経由して Cisco SEA クラウドポータルに到達できる必要があります。ネットワークトポロジがこの到達可能性を提供していることを確認します。

手順

ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。

ステップ 2 [External Services] をクリックします。

ステップ 3 [Secure Equipment Access Cloud] ペインで、次のように入力します。

表 3 : [Secure Equipment Access Cloud] ペイン

フィールド	説明
Cluster access type	API キーオプションを選択します。 • [Manual]：API キーを Cisco SEA クラウドポータルからコピーして、手動で入力します。 • [Auto]：Cisco SEA クラウドポータルから API キーを自動的に取得します。

フィールド	説明
API Key	（このフィールドは、[Cluster access type] で [Manual] を選択した場合に表示されます。） Cisco SEA クラウドポータルで生成した API キーを入力します。
Select Secure Equipment Access Cluster	（このフィールドは、[Cluster access type] で [Auto] を選択した場合に表示されます。） お使いの Cisco SEA クラウドポータルのアカウントに関連付けられているクラスタ名を選択します。[Connect] をクリックし、Cisco SEA クラウドポータルのログイン情報を使ってログインします。
VPN	デバイスと Cisco SEA クラウドポータル間の到達可能性を提供する VPN。
Proxy	ネットワーク内のデバイスが、デバイスと Cisco SEA クラウドポータル間の接続にプロキシを必要とする場合は、プロキシの IP アドレスを入力します。

ステップ 4 [Save] をクリックします。

API キーに含まれている情報を使用して、Cisco SD-WAN Manager はリモート イメージ ホスティング サーバーの 1 つとしてサーバーを自動的に設定します。このサーバーは、**[Maintenance]** > **[Software Repository]** ページの **[Remote server]** タブに表示されます。Cisco Secure Equipment ソリューションへのオンボードプロセス （4 ページ）を参照してください。

SEA 機能を使用した設定グループプロファイルの作成

始める前に

[Configuration] > **[Configuration Groups]**ページで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

ステップ 2 その他のプロファイルで SEA 機能を作成して設定します。

1. この機能の名前と説明を入力します。

表 *4*：名前と説明

フィールド	説明
Name	機能の名前。
Description	任意で説明を追加します。

2. 仮想ポートグループ（VPG）7 を使用して、Cisco SEA エージェントとホストデバイスの物理インターフェイス間の接続を設定します。これは、Cisco SEA エージェントが Cisco SEA クラウドポータルに到達できるようにするために必要です。

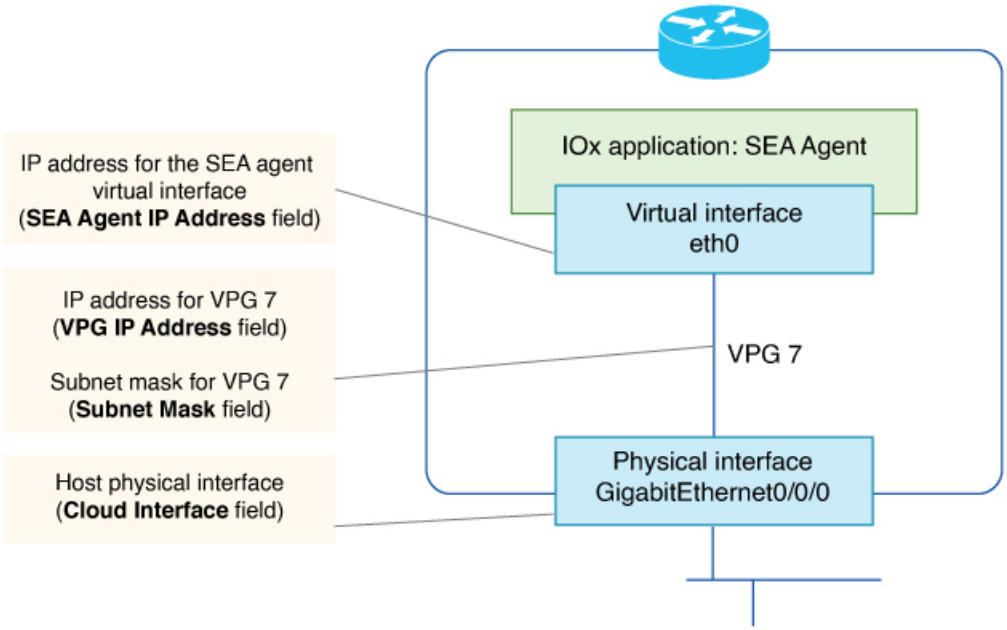


表 *5*：基本設定

フィールド	説明
VPG IP Address	仮想ポートグループ（VPG）7に割り当てる IP アドレス。この VPG は、Cisco SEA エージェントとホストデバイスの物理インターフェイス間の仮想リンクです。 例：10.100.1.1
Subnet Mask	Cisco SEA クラウドポータルに接続する VPG インターフェイス 7 のサブネットマスク。このフィールドと [VPG IP Address] によって、 VPG 7 ネットワークのアドレス空間が定義されます。 例：255.255.252.0

フィールド	説明
SEA Agent IP Address	VPG 7 にマッピングするために Cisco SEA クラウドエージェントに割り当てる IP アドレス。[VPG IP Address] と [Subnet Mask] で定義したアドレス空間内のアドレスを入力します。 例：10.100.1.2
Cloud Interface	SD-Routing ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。 デバイスが Cisco SEA クラウドポータルに接続するために使用する物理インターフェイスを入力します。インターフェイスタイプにはセルラーを含めることができます。 例：GigabitEthernet0/0/0 例：Cellular0/1/0 （注） SD-WAN ソリューション（SD-Routing ソリューションではない）を設定するデバイスの場合、VPG はホストデバイスと Cisco SD-WAN Manager 間の制御接続に使用されるホストインターフェイスに自動的に接続されます。

3. 必要に応じて、アセットに接続するためのアセットネットワークを 1 つ以上設定します。

表 *6:* アセット アクセス ネットワーク（任意）

フィールド	説明
Add Access Network	最大3つのアセットネットワークの接続を設定します。各アセットネットワークには、複数のアセットを含めることができます。
Service VPN	（SD-WAN ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。） アセットが複数の異なるサービス VPN に分散している場合は、必要に応じて各サービス VPN をここに追加します。 （注） （a）Cisco SEA クラウドポータルとの接続に使用されるサービス VPN と、（b）ここで設定する各サービス VPN 間の接続を提供するようにルートリークを設定します。
Asset Interface	（SD-Routing ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。） デバイスがアセットネットワークに接続するために使用している物理インターフェイス。

フィールド	説明
VPG IP Address	ルータの VPG インターフェイスに割り当てる IP アドレス。
SEA Agent IP Address	ルータのそれぞれの VPG インターフェイスにマッピングするために、SEA アセットエージェントに割り当てる IP アドレス。このアドレスは、アセットの VPG インターフェイスと同じネットワーク内にある必要があります。
Subnet Mask	VPG サブネットマスク。
Action	削除オプションを使用するとテーブルの行が削除され、アセットネットワークの設定が削除されます。

4. Cisco SEA ポータルのドメイン名を解決できるネットワーク内の DNS サーバーを設定します。

表 7: ネームサーバー

フィールド	説明
Add Name Server	Cisco SEA ポータルのドメイン名を解決できるネットワーク内の DNS サーバーを設定します。[Add Name Server] をクリックすると、ネームサーバーが追加されます。 Cisco SEA ポータルのドメイン名については、「Network ports and protocols」[英語] を参照してください。 これは必須フィールドです。ネームサーバーを設定しないと、設定を保存できません。 ネームサーバー名の最大数：5
Name Server	ドメインネームサーバーの IP アドレス。
Action	削除オプションを使用するとテーブルの行が削除され、ネームサーバーが削除されます。

次のタスク

「Deploy a configuration group」[英語] も参照してください。

設定グループへの Cisco SEA 機能の追加

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

ステップ 2 [solution] ドロップダウンリストで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択し、このソリューションの設定グループのみを表示します。

ステップ 3 [Configuration Groups] タブをクリックします。

ステップ 4 設定グループを作成する必要がある場合は、『*Cisco Catalyst SD-WAN Configuration Groups*』の「Using Configuration Groups」[英語] で説明されている手順に従います。

ステップ 5 既存の設定グループの場合は、[Add Profile] をクリックして、設定グループに [Other Profile] を追加します。

ステップ 6 設定グループで [Other Profile] ドロップダウンリストを見つけて、Cisco SEA プロファイルを選択します。

Cisco SEA 機能を追加した設定グループの展開

始める前に

- Cisco SEA 機能を追加した設定グループを展開する前に、Cisco Secure Equipment Access との統合でサポートされるプラットフォーム （5 ページ）を参照してください。
- Cisco SEA 機能を追加した設定グループを展開する前に、Cisco SEA エージェントを実行するデバイスごとに、デバイスが Cisco SEA クラウドポータルにネットワーク経由で到達できることを確認してください。これには次の 2 つの手順が必要です。
  1. 設定グループを展開して、Cisco SEA クラウドポータルへの到達可能性を確立します。
  2. 設定グループを展開して、デバイスで Cisco SEA を有効にします。

     前の手順で到達可能性を確立したら、その手順で使用したものと同じ設定グループを変更して Cisco SEA 機能を追加し、その設定グループをデバイスに展開できます。

Cisco Secure Equipment Access との統合の前提条件 （6 ページ）を参照してください。

（注） Cisco SEA 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco SEA クラウドポータルへの到達可能性を確立します。

手順

ステップ 1 『*Cisco Catalyst SD-WAN Configuration Groups*』の「standard configuration group deployment procedure」[英語]に従って、ネットワーク内のデバイスに設定グループを展開します。

ステップ 2 SD-WAN ソリューションタイプのデバイスに展開する場合は、展開時にルータごとにデバイス固有の変数を必要に応じて入力します。

SD-Routing ソリューションタイプのデバイスに展開する場合は、この手順をスキップしてください。

ステップ 3 デバイスに Cisco SEA アプリケーションをインストールする際に進行状況をモニターするには、インストールのログメッセージを表示します。

1. 右上近くにあるタスクリストボタンをクリックします。
2. [Deploy configuration group] タスクをクリックします。

   この操作により、各デバイスに関する展開の進行状況を示すページが開きます。
3. デバイスの横にある [Action] 列のログアイコンをクリックします。

   [View Logs] ペインが開き、そのデバイスに関する展開の進行状況が表示されます。展開が完了し、デバイスと Cisco SEA クラウドポータルとの接続が確立されると、「Config Group successfully deployed to device,」といった成功メッセージがログに表示されます。

   Cisco SEA 機能を追加した設定グループをはじめてデバイスに展開すると、デバイスで Cisco SEA アプリケーションのインストールがトリガーされます。デバイスで Cisco SEA アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco SEA ソリューションの一部として動作します。

Cisco SD-WAN Manager が Cisco Secure Equipment Access クラウドポータルに接続していることを確認する

Cisco SEA 機能を追加した設定グループを作成した場合、その設定グループをデバイスに展開すると、デバイスで Cisco SEA アプリケーションのインストールがトリガーされます。デバイ

スで Cisco SEA アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco SEA ソリューションの一部として動作します。

始める前に

Cisco SEA 機能を追加した設定グループを 1 つ以上のデバイスに展開します。Cisco SEA 機能を追加した設定グループの展開 （13 ページ）を参照してください。

手順

ステップ 1 Cisco SEA クラウドポータルにログインします。

ステップ 2 デバイスリストを表示します。詳細については、Cisco DevNet サイトの Cisco Secure Equipment Access のマニュアル [英語] を参照してください。

CLI を使用して Cisco Secure Equipment Access アプリケーションがデバイスで動作していることを確認する

この検証方法は、SD-WAN または SD-Routing ソリューションのデバイスに適用できます。

始める前に

Cisco Secure Equipment Access 機能を追加した設定グループを 1 つ以上のデバイスに展開します。Cisco SEA 機能を追加した設定グループの展開 （13 ページ）を参照してください。

手順

ステップ 1 Cisco Secure Equipment Access アプリケーションを実行しているデバイスで、次のコマンドを実行します。

```
Device# show iox-service
```

ステップ 2 前のステップのコマンドの出力に基づいて、次のいずれかを実行します。

- コマンド出力に IOxman サービスが実行中であることが示されている場合は、次の手順に進みます。
- コマンド出力に IOxman サービスが実行中でないと表示される場合は、Cisco Secure Equipment Access アプリケーションが正しく動作していないことを示します。アプリケーションを再インストールします。Cisco SEA 機能を追加した設定グループの展開 （13 ページ）を参照してください。

ステップ 3 同じデバイスで、次のコマンドを実行します。実行中の状態であるとコマンド出力に表示される場合は、Cisco Secure Equipment Access アプリケーションが正しく動作していることを示します。

```
Device# show app-hosting detail appid sea
```

例

この例では、Cisco Secure Equipment Access アプリケーションがインストールされ、動作しています。ここではコマンド出力が省略されることに注意してください。

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

Device# show app-hosting detail appid sea
App id                 : sea
Owner                  : iox
State                  : RUNNING
...
```

デバイス上の Cisco Secure Equipment Access アプリケーションのモニター

始める前に

Cisco Secure Equipment Access 機能を追加した設定グループを 1 つ以上のデバイスに展開します。Cisco SEA 機能を追加した設定グループの展開 （13 ページ）を参照してください。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Devices]** の順に選択します。

ステップ 2 SD-WAN ソリューションの対象デバイス名をクリックします。

（注）
このモニタリング方法は、SD-WAN ソリューションのデバイスには適用できますが、SD-Routing ソリューションのデバイスには適用できません。

ステップ 3 [Real Time] タブをクリックします。

ステップ 4 [Device Options] フィールドに次のいずれかのアプリケーション ホスティング コマンドを入力して、デバイスで実行されている Cisco Secure Equipment Access アプリケーションのリソース使用状況やその他の詳細を表示します。

- アプリケーション ホスティングの詳細

- アプリケーション ホスティングの稼働率
- アプリケーション ホスティング ネットワークの稼働率
- アプリケーション ホスティング ストレージの使用率
- アプリケーション ホスティング プロセス
- アプリケーション ホスティングでアタッチされるデバイス
- アプリケーション ホスティング ネットワーク インターフェイス
- アプリケーション ホスティング ゲスト ルート

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。